DISA JIEO Standards Analysis **4 OCT 99**

Certificate Request

References:

RFC 1738, Uniform Resource Locators (URL)
RFC 2104, HMAC: Keyed-Hashing for Message Authentication
RFC 2459, Internet X.509 Public Key Infrastructure Certificate and CRL Profile
RFC 2511, Internet X.509 Certificate Request Message Format
RFC 2630, Cryptographic Message Syntax
MISPC, Minimum Interoperability Specification for PKI Components, Version 1
DOD, DOD Medium Assurance PKI Functional Specification (DRAFT) version 0.3 (20 OCT 98)

Implementation under analysis:

Analysis Date:

REQUIREMENT FROM STANDARDS	MET (Y/N/na)	NOTES
Is a CertRequest value constructed? [RFC 2511: 2]		
Can multiple certificate request messages be sent together? [RFC 2511: 3]		
Does each certificate request message contain a certReq field? [RFC 2511: 3]		
Does each CertRequest have an identifier? [RFC 2511: 5]		
Does each CertRequest indicate with which fields the certificate is to be issued? [RFC 2511: 5]		
Can the version field be requested? [RFC 2511: 5]		
Can the serialNumber field be requested? [RFC 2511: 5]		
Can the signingAlg field be requested? [RFC 2511: 5]		
Can the issuer field be requested? [RFC 2511: 5]		
Can the validity field be requested? [RFC 2511: 5]		
Can the subject field be requested? [RFC 2511: 5]		
Can the Subject Public Key field requested? [RFC 2511: 5]		
Can the issuer unique identifier field be requested? [RFC 2511: 5]		
Can the subject unique identifier field be requested? [RFC 2511: 5]		
Can extensions be requested? [RFC 2511: 5]		
Can a CertRequest provide attributes that affect the certificate's issuance? [RFC 2511: 5]		

REQUIREMENT FROM STANDARDS	MET (Y/N/na)	NOTES
Can the CertRequest include the regToken control? [RFC 2511: 6]		
Is UTF8 used to encode the value of regToken? [RFC 2511: 6.1]		
Can the Certificate Authority (CA) generate a reqToken value to be used by the subscriber? [RFC 2511: 6.1]		
Can the CA and subscriber obtain the same regToken value from another source? [RFC 2511: 6.1]		
Does the CA use the regToken value to confirm the subject's identity? [RFC 2511: 6.1]		
Can the regToken control be used to initialize a new End Entity (EE) into the PKI system? [RFC 2511: 6.1]		
Can the CertRequest include the authenticator control? [RFC 2511: 6]		
Can the subscriber generate the authenticator control value? [RFC 2511: 6.2]		
Can the CA generate the authenticator control value? [RFC 2511: 6.2]		
Is UTF8 used to encode the value of authenticator? [RFC 2511: 6.2]		
Do the subscriber and CA retain copies of the authenticator value?		
Does the CA use the authenticator value to confirm the subject's identity in an ongoing basis? [RFC 2511: 6.2]		
Can the CertRequest include the pkiPublicationInfo control? [RFC 2511: 6]		
If the requestor chooses the dontPublish action, is pubInfos not included in pkiPublicationInfo? [RFC 2511: 6.3]		
Can the CA process the pkiPublicationInfo field? [RFC 2511: 6.3]		
If the pleasePublish action is indicated and pubInfos is absent, does the CA assume the dontCare method? [RFC 2511: 6.3]		
If the pkiPublicationInfo field is not present does the CA publish the certificate in the repository? [RFC 2511: 6.3]		
If the dontPublish action is indicated, does the CA not publish the certificate in the repository? [RFC 2511: 6.3]		
If the pleasePublish action and the dontCare pubMethod are indicated, does the CA publish the certificate in the repository? [RFC 2511: 6.3]		
If the pleasePublish action, the dontCare and x500 pubMethod are indicated, does the CA publish the certificate in the repository and the IP address given in pubLocation? [RFC 2511: 6.3, RFC 2459: 4.2.1.7]		
If the pleasePublish action, the dontCare and web pubMethod are indicated, does the CA publish the certificate in the repository and the URL given in pubLocation? [RFC 2511: 6.3, RFC 2459: 4.2.1.7]		
If the pleasePublish action, the dontCare and ldap pubMethod are indicated, does the CA publish the certificate in the repository and the IP address given in pubLocation? [RFC 2511: 6.3, RFC 2459: 4.2.1.7]		
Can the CertRequest include the pkiArchiveOptions control? [RFC 2511: 6]		

REQUIREMENT FROM STANDARDS	MET (Y/N/na)	NOTES
If the requestor does not wish to archive it's private key, does it set archiveRemGenPrivKey to FALSE? [RFC 2511: 6.4]		
If the requestor does wish to archive it's private key, does it set archiveRemGenPrivKey to TRUE? [RFC 2511: 6.4]		
If archiving it's private key, does the requestor place the encrypted private key into the envelopedData encryptedContentInfo encryptedContent OCTET STRING? [RFC 2511: 6.4, RFC 2630: 6.1]		
Can the requestor indicate the intended algorithm for which the encValue will be used (intenedeAlg field)? [RFC 2511: 6.4]		
Can the requestor indicate the symmetric algorithm used to encrypt the value (symmAlg field)? [RFC 2511: 6.4]		
Can the requestor include the encrypted symmetric key used to encrypt the value (encSymmKey field)? [RFC 2511: 6.4]		
Can the requestor indicate the algorithm used to encrypt the symmetric key (keyAlg field)? [RFC 2511: 6.4]		
Can the requestor provide a brief description or identifier of the encValue content (valueHint field)? [RFC 2511: 6.4]		
Does the requestor include the encrypted value of the private key in the encValue field? [RFC 2511: 6.4]		
Can the requestor send information on how to regenerate its private key in the KeyGenParameters field? [RFC 2511: 6.4]		
Can the CA process the pkiArchiveOptions field and archive the subscriber's private key? [RFC 2511: 6.4]		
Can the CertRequest include the oldCertID control? [RFC 2511: 6]		
Does the requestor provide the issuer's name and the serial number of the certificate to be updated with this control? [RFC 2511: 6.5]		
Is the CA able to process an update of the certificate indicated by the oldCertID control? [RFC 2511: 6.5]		
Can the CertRequest include the protocolEncrKey control? [RFC 2511: 6]		
Does the requestor provide the public key and identify the algorithm with which the key is used? [RFC 2511: 6.6, RFC 2459: 4.1, 4.1.2.7]		
Does the CA use the key indicated by the protocolEncrKey control to encrypt its response to the certificate request message? [RFC 2511: 6.6]		
Can the CA use the key indicated by the protocolEncrKey control to encrypt information it is sending to the subscriber? [RFC 2511: 6.6]		
Can the CA use the key indicated by the protocolEncrKey control to encrypt a private key it is providing to the subscriber? [RFC 2511: 6.6]		
Can a proof of possession (POP) value be calculated? [RFC 2511: 2, 3]		
Can the certificate request message contain a POP field? [RFC 2511: 3]		

REQUIREMENT FROM STANDARDS	MET (Y/N/na)	NOTES
Is private key proof of possession required prior to issuing a certificate binding the public key to a requestor? [RFC 2511: 4]		
Can the Registration Authority (RA) forward the EE's certificate request and POP unaltered to the CA? [RFC 2511: 4]		
Can the RA verify POP? [RFC 2511: 4]		
Can the RA send confirmation to the CA that it has verified POP? [RFC 2511: 4]		
If the RA is not sending confirmation of POP verification, is the raVerified field set to NULL? [RFC 2511: 4.3]		
Is the ProofOfPossession field not used if the CA uses out-of-band POP enforcement methods? [RFC 2511: 4]		
For signature keys or multipurpose keys does the EE sign a value to prove possession of the private key? [RFC 2511: 4, 4.1, 4.4]		
For signature keys or multipurpose keys: If the CertReqMsg does not request a certificate containing the subject and publicKey fields, is the poposkInput present and is the signature (using "algorithmIdentifier") computed on the DER-encoded value of poposkInput? [RFC 2511: 4.4]		
Does the receiving CA/RA confirm the authenticity of the request by confirming the signature computed on poposkInput? [RFC 2511: 4]		
For signature keys or multipurpose keys: If the CertReqMsg requests that the certificate contains the subject and publicKey fields is the poposkInput omitted and is the signature computed on the DER-encoded value of CertReqMsg certReq? [RFC 2511: 4.4]		
Does the receiving CA/RA confirm the authenticity of the request by confirming the signature computed on CertReqMsg certReq? [RFC 2511: 4]		
For signature keys or multipurpose keys: If established, is the authenticated GeneralName of the sender provided in the POPOSigningKeyInput authInfo field? [RFC 2511: 4.4]		
Does the receiving CA/RA confirm the authenticity of the request by confirming the GeneralName of the sender provided in the POPOSigningKeyInput authInfo field? [RFC 2511: 4]		
For signature keys or multipurpose keys: If no authenticated GeneralName for the sender exists, is a password-based Message Authentication Code (MAC) on the DER-encoded value of the publicKey field provided in the POPOSigningKeyInput authInfo field? [RFC 2511: 4.4, RFC 2104: 2]		
For signature keys or multipurpose keys: Is the PasswordBasedMAC (1.2.840.113533.7.66.13) algorithm used for to calculate the MAC? [RFC 2511: 4.4]		

REQUIREMENT FROM STANDARDS	MET (Y/N/na)	NOTES

For signature keys or multipurpose keys: Does the PKMACValue value field consist of the following ASN.1 sequence (PBMParameter)? [RFC 2511: 4.4, 4.4.1]:
 	
`salt OCTET STRING,`
`owf AlgorithmIdentifier,`
`iterationCount INTEGER,`
`-- number of times the OWF is applied`
`mac AlgorithmIdentifier`		

Is the owf AlgorithmIdentifier 1.3.14.3.2.26 (SHA-1)? [RFC 2511: 4.4.1]		
Is the mac AlgorithmIdentifier 1.3.6.1.5.5.8.1.2 (HMAC-SHA1)? [RFC 2511: 4.4.1]		
Does the publicKeyMAC computation require the input of a shared secret known to the receiving CA/RA and the sending EE? [RFC 2511: 4.4.1, App. A]		
Does the receiving CA/RA confirm the authenticity of the request by comparing the publicKeyMAC value received, against a hash value it generates using the shared secret, and the data and OIDs provided by PKMACValue value field? [RFC 2511: 4, 4.4.1, App. A, RFC 2104: 2]		
For signature keys or multipurpose keys: Is the public key and algorithm OID provided in the POPOSigningKeyInput publicKey field? [RFC 2511: 4.4]		
For key encipherment keys, can the EE provide its private key, encrypted by the CA/RA's public key, in the POPOPrivKey thisMessage field? [RFC 2511: 4.2, 4.4]		
Does the CA/RA authenticate the EE's POP on receipt of the EE's private key? [RFC 2511: 4.2, 4.4]		
For key encipherment keys, can the EE set SubsequentMessage to 1 to request a challenge-response exchange with the receiving CA/RA? [RFC 2511: 4.2, 4.4]		
To establish EE POP, can the CA/RA response to a SubsequentMessage value of 1 by issuing a random challenge to the EE? [RFC 2511: 4.2, 4.4]		
Can the EE respond to the CA/RA's challenge? [RFC 2511: 4.2, 4.4]		
For key encipherment keys, can the EE set SubsequentMessage to 0 to request the issued certificate be encrypted using the EE's public key? [RFC 2511: 4.2, 4.4]		
In response to a SubsequentMessage value of 0, can the CA issue the EE an encrypted certificate? [RFC 2511: 4.2, 4.4]		
On decryption of the received encrypted certificate, can the EE send a confirmation message to the CA/RA? [RFC 2511: 4.2, 4.4]		
Can the CA/RA accept the confirmation message as the EE's POP? [RFC 2511: 4.2, 4.4]		

REQUIREMENT FROM STANDARDS	MET (Y/N/na)	NOTES
For key agreement keys, can the EE provide its private key, encrypted by the CA/RA's public key, in the POPOPrivKey thisMessage field? [RFC 2511: 4.3, 4.4]		
Does the CA/RA authenticate the EE's POP on receipt of the EE's private key? [RFC 2511: 4.3, 4.4]		
For key agreement keys, can the EE set SubsequentMessage to 1 to request a challenge-response exchange with the receiving CA/RA? [RFC 2511: 4.3, 4.4]		
To establish EE POP, can the CA/RA response to a SubsequentMessage value of 1 by issuing a random challenge to the EE? [RFC 2511: 4.3, 4.4]		
Can the EE sent a response constructed using a shared secret key? [RFC 2511: 4.3, 4.4, App. A]		
For key agreement keys, can the EE set SubsequentMessage to 0 to request the issued certificate be encrypted? [RFC 2511: 4.3, 4.4]		
In response to a SubsequentMessage value of 0, can the CA issue the EE a certificate encrypted using a shared secret key? [RFC 2511: 4.3, 4.4, App. A]		
Can the EE decrypt the received encrypted certificate using a shared secret key, and then send a confirmation message to the CA/RA? [RFC 2511: 4.3, 4.4, App. A]		
Can the CA/RA accept the confirmation message as the EE's POP? [RFC 2511: 4.3, 4.4]		
For key agreement keys, if the EE has the CA's Diffie-Hellman (DH) certificate and parameters, and the certificate request has both the subject and publicKey fields present, can the EE MAC the certificate request using a DH shared secret key derived from the EE's private DH key and the CA's public DH key? [RFC 2511: 4.3, 4.4, App. A, RFC 2104: 2]		
Does the CA accept this MAC value as the EE's POP? [RFC 2511: 4.3, 4.4, App. A, RFC 2104: 2]		
Can the certificate request message contain additional registration information? [RFC 2511: 2, 3]		
Does the CA/RA not include the information present in the CertReqMsg regInfo field in the certificate? [RFC 2511: 3]		
When name-value pairs are present, are they structured as: `[name?value][%name?value]*%` and then encoded as an OCTET STRING? [RFC 2511: App. B.1]		
Are reserved characters encoded using "%" and two hexadecimal digits? [RFC 2511: App. B.1, RFC 1738: 2.2]		
Is "version" the text string used to identify that the version of this variation of regInfo is being provided? [RFC 2511: App. B.1]		
Is "corp_company" the text string used to identify that the company affiliation of subscriber is being provided? [RFC 2511: App. B.1]		

REQUIREMENT FROM STANDARDS	MET (Y/N/na)	NOTES
Is "org_unit" the text string used to identify that the organizational unit affiliation of subscriber is being provided? [RFC 2511: App. B.1]		
Is "mail_firstName" the text string used to identify that a personal name component of subscriber is being provided? [RFC 2511: App. B.1]		
Is "mail_middleName" the text string used to identify that a personal name component of subscriber is being provided? [RFC 2511: App. B.1]		
Is "mail_lastName" the text string used to identify that a personal name component of subscriber is being provided? [RFC 2511: App. B.1]		
Is "mail_email" the text string used to identify that the subscriber's email address is being provided? [RFC 2511: App. B.1]		
Is "jobTitle" the text string used to identify that the job title of subscriber is being provided? [RFC 2511: App. B.1]		
Is "employeeID" the text string used to identify that the employee identification number or string of the subscriber is being provided? [RFC 2511: App. B.1]		
Is "mailStop" the text string used to identify that the subscriber's mail stop is being provided? [RFC 2511: App. B.1]		
Is "issuerName" the text string used to identify that the name of the CA is being provided? [RFC 2511: App. B.1]		
Can the EE provide the name in X.500 directory form? [RFC 2511: App. B.1.1]		
Can the CA/RA process the name in X.500 directory form? [RFC 2511: App. B.1.1]		
Can the EE provide the name in E-mail address form? [RFC 2511: App. B.1.1]		
Can the CA/RA process the name in E-mail address form? [RFC 2511: App. B.1.1]		
Can the EE provide the name in DNS form? [RFC 2511: App. B.1.1]		
Can the CA/RA process the name in DNS form? [RFC 2511: App. B.1.1]		
Can the EE provide the name in URI form? [RFC 2511: App. B.1.1]		
Can the CA/RA process the name in URI form? [RFC 2511: App. B.1.1]		
Can the EE provide the name in IP address? [RFC 2511: App. B.1.1]		
Can the CA/RA process the name in IP address? [RFC 2511: App. B.1.1]		
Can the EE provide the name in other name form? [RFC 2511: App. B.1.1]		
Can the CA/RA process the name in other name form? [RFC 2511: App. B.1.1]		
Is "subjectName" the text string used to identify that the name of the Subject is being provided? [RFC 2511: App. B.1]		
Can the EE provide the name in X.500 directory form? [RFC 2511: App. B.1.1]		

REQUIREMENT FROM STANDARDS	MET (Y/N/na)	NOTES
Can the CA/RA process the name in X.500 directory form? [RFC 2511: App. B.1.1]		
Can the EE provide the name in E-mail address form? [RFC 2511: App. B.1.1]		
Can the CA/RA process the name in E-mail address form? [RFC 2511: App. B.1.1]		
Can the EE provide the name in DNS form? [RFC 2511: App. B.1.1]		
Can the CA/RA process the name in DNS form? [RFC 2511: App. B.1.1]		
Can the EE provide the name in URI form? [RFC 2511: App. B.1.1]		
Can the CA/RA process the name in URI form? [RFC 2511: App. B.1.1]		
Can the EE provide the name in IP address? [RFC 2511: App. B.1.1]		
Can the CA/RA process the name in IP address? [RFC 2511: App. B.1.1]		
Can the EE provide the name in other name form? [RFC 2511: App. B.1.1]		
Can the CA/RA process the name in other name form? [RFC 2511: App. B.1.1]		
Is "validity" the text string used to identify that the certificate validity interval is being provided? [RFC 2511: App. B.1]		
Can the EE provide a notbefore time? [RFC 2511: App. B.1.1]		
Can the CA/RA issue a certificate that is valid from the issuance date or the notbefore time, whichever is later? [MISPC: 3.5.1]		
Can the EE provide a notafter time? [RFC 2511: App. B.1.1]		
Can the CA/RA issue a certificate that expires on or before the notafter time? [MISPC: 3.5.1]		
Is UTC time in the form YYYYMMDD[HH[MM[SS]]] where HH, MM, and SS default to 00 and are omitted if the previous time is 00? [RFC 2511: App. B.1.1]		
Is a web interface available to EE's to request certificates over HTTP over SSL? [DOD: 3.6.1.1.1, App. E]		
Can an EE submit a PKCS #10 formatted certificate request? [DOD: 3.6.1.1.1, App. E]		
Is the PKCS #10 request Base 64 encoded with both a “begin” header and an “end” trailer? [DOD: 3.6.1.1.1, App. E]		
Can an EE submit a PKCS #10 request via a web form? [DOD: 3.6.1.1.1, App. E]		

Other information:

Findings:

Recommendations for Standards Work: